

IMPLEMENTASI WEB VULNERABILITY SCANNER
SEBAGAI ADD ONS MOZILLA FIREFOX

SKRIPSI



Oleh :

ARDI MARTONO

0734010030

JURUSAN TEKNIK INFORMATIKA
FAKULTAS TEKNOLOGI INDUSTRI
UNIVERSITAS PEMBANGUNAN NASIONAL “VETERAN”
JAWA TIMUR
2011

IMPLEMENTASI WEB VULNERABILITY SCANNER
SEBAGAI ADD ONS MOZILLA FIREFOX

SKRIPSI

Diajukan Untuk Memenuhi Sebagian Persyaratan
Dalam Memperoleh Gelar Sarjana Komputer
Jurusan Teknik Informatika



Oleh :

ARDI MARTONO
0734010030

JURUSAN TEKNIK INFORMATIKA
FAKULTAS TEKNOLOGI INDUSTRI
UNIVERSITAS PEMBANGUNAN NASIONAL "VETERAN"
JAWA TIMUR
2011

ABSTRAKSI

Ardi Martono, 2011. Implementasi Web Vulnerability Scanner sebagai Add Ons Mozilla Firefox (dibimbing oleh Nur Cahyo Wibowo,S.Kom.,M.Kom dan Achmad Junaidi, S.Kom)

Internet pada era ini, sudah menyebar di semua kalangan masyarakat. Sehingga para pengguna internet masih belum memperhatikan segi keamanan dari sebuah website, khususnya mengenai penyerangan SQL Injection dan XSS Injection. Sehingga perlu dikembangkan aplikasi Web Vulnerability Scanner sebagai Add Ons Mozilla Firefox dengan model pendeteksian yang bisa mengetahui kelemahan website tersebut. Sehingga website yang masih mempunyai kelemahan terhadap SQL Injection dan XSS Injection dapat segera di deteksi dan diperbaiki.

Dalam Tugas akhir ini, aplikasi dirancang dengan bahasa pemrograman JavaScript dan HTML. Aplikasi ini mencari perbedaan antara proses URL asli dan URL setelah mengalami pendeteksian. Aplikasi tersebut melakukan scanning secara Online. Hasil scanning ditampilkan langsung oleh aplikasi untuk dipergunakan serta untuk menambah wawasan tentang pengemasan aplikasi secara sederhana.

Dilakukan ujicoba terhadap aplikasi ini dengan beberapa website. Dari beberapa website yang diacak untuk dilakukan testing dan ditemukan rata-rata hasil proses lebih banyak dibandingkan hasil akhir dari perolehan pendeteksian kelemahan.

Keyword: Web Vulnerability Scanner, XSS Injection dan SQL Injection.

KATA PENGANTAR

Alhamdulillah, dengan mengucapkan puji dan syukur kehadiran Allah SWT atas rahmat dan hidayah-Nya sehingga penulis dapat menyelesaikan tugas akhir ini dengan judul “IMPLEMENTASI WEB VULNERABILITY SCANNER SEBAGAI ADD ONS MOZILLA FIREFOX” yang merupakan persyaratan dalam memperoleh gelar Sarjana Komputer di Universitas Pembangunan Nasional “VETERAN” Jatim.

Penulis mengucapkan terima kasih yang sebesar-besarnya kepada pihak-pihak yang telah membantu baik materiil maupun dorongan spirituil untuk menyelesaikan penulisan kerja praktek ini, terutama kepada:

1. Orang Tua dan keluarga atas motivasi dan doanya sehingga semua yang dikerjakan dapat berjalan lancar.
2. Bapak Achmad Junaidi, S.Kom, dan Bapak Nur Cahyo Wibowo, S.Kom,.M.Kom. selaku Dosen Pembimbing yang telah meluangkan waktu untuk memberikan bimbingan selama proses pelaksanaan Tugas Akhir penulis.
3. Bapak Prof. Dr. Ir. Teguh Soedarto, MP, selaku Rektor UPN “Veteran” Jatim.
4. Bapak Ir. Sutiyono, MT selaku DEKAN FTI UPN “VETERAN” Jatim.
5. Ibu Dr. Ir. Ni Ketut Sari, MT. Selaku Kepala Jur. Teknik Informatika, FTI UPN “VETERAN” Jatim
6. Special to: Aditya Wardana yang banyak sekali memberi motivasi dan membantu saya dalam menemukan solusi didalam pengerjaan tugas akhir ini

dan laptop Lenovo Intel Centrino Core I 3 yang selalu setia menemani saya untuk mengerjakan ini semua.

7. Dosen-dosen Teknik Informatika dan Sistem Informasi, staff dan segenap akademika UPN “VETERAN” Jatim.
8. Teman-teman baik saya yang setia menemani mencari inspirasi gigih, Nanang, Yudith, Yursa, Malik, Sueb, Trea, Faisol, Novan, Rizal, Tobib, Candr a, Bayu, Adi, Rezky, Dadus, Rahendra, Erik, Adit.

Penulis menyadari sepenuhnya masih banyak terdapat kekurangan dalam penulisan Tugas Akhir ini. Oleh sebab itu kritik serta saran yang membangun dari pembaca sangat membantu guna perbaikan dan pengembangan di masa yang akan datang.

Akhirnya dengan ridho Allah penulis berharap semoga Tugas Akhir ini dapat memberikan manfaat bagi pembaca sekalian terutama mahasiswa di bidang komputer.

Surabaya, 09 Oktober 2011

Penulis

DAFTAR ISI

	Halaman
HALAMAN JUDUL	
LEMBAR PENGESAHAN	
LEMBAR PENGESAHAN DAN PERSETUJUAN	
KETERANGAN REVISI	
MOTTO	
KATA PENGANTAR	i
DAFTAR ISI	iii
DAFTAR TABEL	vi
DAFTAR GAMBAR	vii
ABSTRAKSI	xvi
BAB I PENDAHULUAN	1
1.1 Latar Belakang Masalah	1
1.2 Perumusan Masalah	2
1.3 Batasan Masalah	3
1.4 Tujuan	3
1.5 Manfaat Sistem Bagi Pengguna	3
1.6 Metodologi	4
BAB II TINJAUAN PUSTAKA.....	7
2.1 Sejarah Website dan Browser	6
2.2 Injeksi SQL	8
2.3 Injeksi XSS	8
2.4 Pengertian Scanning.....	13
2.5 Contoh Penyerangan XSS.....	14
2.6 Pembuatan Add-Ons Firefox.....	17
BAB III PERANCANGAN	21
3.1 Desain Sistem	21
3.2 Perancangan Sistem	23
3.3 Perancangan Input	23

3.4 Perancangan Proses	24
3.4.1 Proses Scanning	24
3.5 Perancangan Antar Muka	33
3.5.1 Blok Arsitektur Sistem.....	33
3.5.2 Tampilan Antar Muka Aplikasi	34
3.5.3 Perancangan Uji Coba	35
BAB IV IMPLEMENTASI	38
4.1 Implementasi Sistem	38
4.1.1 Interface utama	38
4.1.2 Interface Scanning SQL Injection pada URL	39
4.1.3 Interface Scanning SQL Injection pada PAGE	41
4.1.4 Interface Scanning SQL Injection pada SITE	43
4.1.5 Interface Scanning XSS Injection pada URL	47
4.1.6 Interface Scanning XSS Injection pada PAGE	48
4.1.7 Interface Scanning XSS Injection pada SITE	51
4.1.8 Interface Get Info about Domain Website	54
4.1.9 Interface Get Info about Client Connection	56
4.1.10 Interface Get Information about Cookie	58
4.1.11 Interface Scanning Terakhir	60
BAB V PENGUJIAN DAN ANALISIS	61
5.1 Lingkup Pengujian	61
5.2 Uji Coba	61
5.2.1 Aplikasi Web Vulnerability Scanner	61
5.2.2 Proses Scanning Secara Online	62
1) Scanning SQL Injection pada URL	64
2) Scanning SQL Injection pada PAGE	66
3) Scanning SQL Injection pada SITE secara cepat	68
4) Scanning SQL Injection pada SITE secara penuh	70
5) Scanning XSS Injection pada URL	72
6) Scanning XSS Injection pada PAGE	74

7) Scanning XSS Injection pada SITE secara cepat	76
8) Scanning XSS Injection pada SITE secara penuh	78
9) Get Info about Domain Website	81
10) Get Info about Client Connection	82
11) Get Information about Cookie	83
5.3 Analisis	84
BAB VI PENUTUP	86
6.1 Kesimpulan	86
6.2 Saran	86
DAFTAR PUSTAKA	

DAFTAR TABEL

	Halaman
Tabel 5.1 Daftar alamat website uji coba	63
Tabel 5.2 Hasil Scanning pada berbagai website.....	83

DAFTAR GAMBAR

	Halaman
Gambar 2.1 Informasi yang valid dari website (SQL).....	10
Gambar 2.2 Informasi yang tidak valid dari website (SQL).....	10
Gambar 2.3 Informasi yang valid dari website (XSS).....	12
Gambar 2.4 Informasi yang tidak valid dari website .(XSS).....	13
Gambar 2.5 Coding XML register ESET.....	15
Gambar 2.6 Coding PHP penyimpanan LOG.....	15
Gambar 2.7 Fake Register ESET.....	16
Gambar 2.8 Hasil LOG pada fake register.....	17
Gambar 2.9 Komponen pendukung Add-Ons.....	18
Gambar 2.10 Coding XML pada browser.xul.....	18
Gambar 2.11 Komponen javascript pendukung	19
Gambar 2.12 Tampilan icon pendukung.....	19
Gambar 2.13 Tampilan instalasi Add-Ons.....	20
Gambar 2.13 Tampilan hasil instalasi.....	20
Gambar 3.1 Perancangan system secara global.....	22
Gambar 3.2 Diagram alur scan XSS.....	25
Gambar 3.3 Diagram alur scan URL.....	27
Gambar 3.4 Diagram alur scan PAGE.....	28
Gambar 3.5 Diagram alur scan SITE.....	30
Gambar 3.6 Diagram alur scan SITE-fast.....	31
Gambar 3.7 Diagram alur info Domain.....	32

Gambar 3.8	Diagram alur informasi client.....	33
Gambar 3.9	Arsitektur Sistem Vulnerability Scanner	33
Gambar 3.10	Tampilan antar muka aplikasi.....	34
Gambar 3.11	Tampilan antar muka hasil scanning.....	35
Gambar 4.1	Tampilan menu utama.....	38
Gambar 4.2	Halaman scanning SQL injection (URL).....	39
Gambar 4.3	Potongan Source Code SQL (URL).....	40
Gambar 4.4	Halaman Scanning SQL (page).....	41
Gambar 4.5	Potongan Source Code SQL (page).....	42
Gambar 4.6	Halaman Scanning SQL (SITE_fast).....	43
Gambar 4.7	Halaman Scanning SQL (SITE_full).....	44
Gambar 4.8	Potongan Code Scanning SQL Site.....	45
Gambar 4.9	Halaman Scanning XSS (URL).....	47
Gambar 4.10	Potongan Code Scanning XSS (URL).....	47
Gambar 4.11	Halaman Scanning XSS (PAGE).....	48
Gambar 4.12	Potongan Code Scanning XSS(PAGE).....	49
Gambar 4.13	Halaman Scanning XSS (SITE_fast).....	51
Gambar 4.14	Halaman Scanning XSS (SITE_full)	51
Gambar 4.15	Potongan kode Scanning XSS site.....	53
Gambar 4.16	Halaman Info Domain	54
Gambar 4.17	Potongan Kode Info Domain	55
Gambar 4.18	Halaman Info Client	56
Gambar 4.19	Potongan Kode Info Client	57
Gambar 4.20	Halaman Get Cookie	58

Gambar 4.21	Potongan Kode Get Cookie	58
Gambar 4.22	Halaman Proses serta Hasil Scanning	59
Gambar 5.1	Tampilan menu utama Addons.	60
Gambar 5.2	Tampilan sebelum diinjeksi oleh SQL (URL).....	64
Gambar 5.3	Tampilan sesudah diinjeksi SQL	64
Gambar 5.4	Tampilan sebelum diinjeksi SQL (page)	65
Gambar 5.5	Tampilan hasil scanning SQL (page)	66
Gambar 5.6	Tampilan setelah diinjeksi	66
Gambar 5.7	Tampilan sebelum diinjeksi SQL SITE (fast).....	67
Gambar 5.8	Tampilan hasil scanning SQL SITE (fast).....	68
Gambar 5.9	Tampilan setelah diinjeksi	68
Gambar 5.10	Tampilan sebelum diinjeksi XSS SITE (FULL)	69
Gambar 5.11	Hasil Scanning XSS Injection pada SITE (full)	70
Gambar 5.12	Tampilan diinjeksi XSS SITE (full)	70
Gambar 5.13	Tampilan sebelum diinjeksi XSS (URL)	72
Gambar 5.14	Hasil scanning XSS.....	73
Gambar 5.15	Tampilan sesudah diinjeksi XSS (URL).....	73
Gambar 5.16	Tampilan sebelum diinjeksi XSS (page)	73
Gambar 5.17	Tampilan hasil scanning XSS (page)	74
Gambar 5.18	Tampilan sesudah diinjeksi XSS(page)	75
Gambar 5.19	Tampilan sebelum diinjeksi XSS SITE (fast).....	76
Gambar 5.20	Tampilan hasil scanning XSS SITE (fast).....	76
Gambar 5.21	Tampilan sesudah diinjeksi XSS SITE (fast)	77
Gambar 5.22	Tampilan sebelum diinjeksi XSS SITE(full).....	78

Gambar 5.23 Hasil scanning XSS SITE (full)	78
Gambar 5.24 Tampilan sesudah diinjeksi XSS SITE (full).....	79
Gambar 5.25 Tampilan Informasi website.....	80
Gambar 5.26 Tampilan info client.....	81
Gambar 5.27 Hasil get cookie.....	82
Gambar 5.28 Perbandingan hasil proses dan hasil scan.....	84

BAB I

PENDAHULUAN

1.1 Latar belakang

Di zaman yang semakin maju seperti sekarang ini perkembangan teknologi internet telah menyebar diseluruh dunia dan kita mengenal telah mengenal yaitu website, dimana website ini sudah meluas diseluruh dunia. Bahkan kita bisa memanfaatkan sebuah teknologi internet untuk mengakses website tersebut dan website tersebut dapat diakses dari berbagai lapisan masyarakat dan usia, sudah bisa menggunakan fasilitas-fasilitas dalam browsing dan download. Dalam hal ini akan membahas tentang internet adalah sistem global dari seluruh jaringan komputer yang saling terhubung menggunakan standar untuk melayani para pengguna diseluruh dunia. Banyak dari para user internet sekarang ini belum menyadari tentang segi keamanannya.

Untuk mengantisipasi adanya tindakan yang merugikan keamanan web, user minimal harus mengetahui beberapa konsep, yaitu memastikan siapa yang diajak untuk berkomunikasi di dunia internet, melindungi data-data yang sangat penting, dan memastikan bahwa web yang diakses aman untuk melakukan browsing, karena apabila user terlalu bebas dalam memberikan informasi, maka hal terbesar adalah pengambilan informasi secara paksa atau lebih dikenal dengan hacking.

Vulnerability scanner adalah alat yang digunakan untuk mengecek sebuah website atau computer pada sebuah jaringan dan situs internet untuk diketahui kelemahan tersebut. Hacker juga biasanya menggunakan port scanner. Port

scanner ini adalah alat untuk melihat port pada komputer tertentu untuk mengakses komputer, dan kadang-kadang akan mendeteksi program nomor versinya.

Sehingga diberikan firewall untuk melindungi komputer dari penyusup dengan membatasi akses ke port, seorang hacker web biasanya menggunakan beberapa metode yang diyakini bisa mendeteksi kelemahan sebuah website yakni dengan metode SQL injection dan metode XSS.

Seiring perkembangan zaman yang semakin pesat terdapat beberapa cara yang lebih sederhana untuk mengemas web vulnerability scanner ini menjadi lebih mudah untuk digunakan yakni dengan menjadikan web tersebut sebagai add-ons sebuah browser. Dimana tujuan dari pembuatan add-ons ini adalah membantu user dan developer website untuk lebih berfokus kepada tingkat keamanan sebuah web.

1.2 Rumusan Masalah

Dari latar belakang yang telah dijelaskan untuk membuat sebuah Add Ons pada browser Mozilla firefox dengan menerapkan proses Vulnerability scanner terdapat rumusan masalah. Adapun beberapa permasalahan yang ada sebagai berikut:

- a. Bagaimana mengemas suatu website kedalam sebuah addons yang menerapkan proses vulnerability scanner yang dapat mendeteksi kelemahan website.
- b. Bagaimana addons tersebut dapat menerapkan pola pendeteksian kelemahan sebuah web terhadap SQL Injection dan XSS (Cross Site Scripting) pada alamat web yang diakses

- c. Bagaimana add-ons tersebut bisa menampilkan hasil dari Vulnerability Scanner untuk dapat diketahui oleh user.

1.3 Batasan Masalah

Dalam penyusunan tugas akhir ini, untuk mengatasi permasalahan yang ada maka disusun beberapa batasan masalah sebagai berikut :

- a. Aplikasi ini mendeteksi alamat URL pada sebuah website yang memiliki kelemahan.
- b. Aplikasi web yang dapat discan adalah alamat website yang dituliskan kepada tag HTML dengan penulisan url yang disesuaikan dengan penulisan html tersebut.
- c. Kelemahan yang dibahas adalah menggunakan SQL injection dan XSS.
- d. Browser yang digunakan adalah Mozilla Firefox 3.6

1.4 Tujuan Penelitian

Adapun tujuan dari penelitian Tugas akhir ini yakni membuat sebuah add-ons vulnerability scanner yang dapat digunakan pada Browser Mozilla Firefox yang membantu developer dan user untuk mengetahui kelemahan sebuah website. Serta memberikan wawasan tentang pengemasan suatu aplikasi kedalam bentuk yang sederhana sehingga lebih efisien dan mudah untuk digunakan.

1.5 Manfaat Penelitian

Manfaat yang dapat diambil dari pembuatan add-ons vulnerability scanner:

- a. Diharapkan untuk selanjutnya penyedia website lebih mementingkan segi keamanan agar data yang dimiliki oleh user tetap terjaga keamanannya

- b. Mengenai segi keamanan tersebut pembuat website minimal memperhatikan script yang akan dibuat agar para hacker tidak dapat menembus web tersebut.
- c. Kepada user dan developer sebagai penambahan wawasan bahwa vulnerability scanner ini tidak hanya dibuat secara web tetapi juga dapat dikemas dengan sederhana menggunakan add-ons pada sebuah browser Mozilla Firefox.

1.6 Metode Penelitian

Metode yang dilaksanakan dalam penelitian ini adalah.

a. Studi Literatur

Dilakukan dengan cara mencari segala macam informasi secara riset keperpustakaan dan mempelajari buku-buku yang berhubungan dengan masalah yang dihadapi, sehingga didapatkan sebuah materi serta literatur yang jelas dan akurat.

b. Pengumpulan dan Analisa Data

Pengumpulan data dilakukan dengan cara : observasi, identifikasi dan klasifikasi melalui studi literatur. Dari pengumpulan data tersebut dapat dilakukan analisa data yaitu dalam proses pembuatan add ons vulnerability scanner pada mozilla firefox.

c. Perancangan Program

Melakukan analisa awal tentang add ons yang akan dibuat yaitu suatu pemecahan masalah yang dilakukan melalui system online dengan cara pembuatan add ons vulnerability scanner pada Mozilla firefox dimana add-ons tersebut dapat mendeteksi kelemahan sebuah website yang

dituliskan pada halaman browser serta memberikan hasil output dari proses hasil scan yang dihasilkan oleh add ons tersebut yang dapat dimanfaatkan.

d. Pengujian dan Analisa

Pengujian dan analisa dimaksudkan untuk mengetahui sejauh mana sistem yang dibuat pada proyek akhir ini dapat berfungsi sesuai dengan proses sistem yang diharapkan.

e. Kesimpulan

Dibuat kesimpulan dari pengujian sistem tugas akhir dengan menguji apakah hasilnya sesuai dengan yang diharapkan pada tujuan tugas akhir.

1.7. Sistematika Penulisan

Dalam laporan tugas akhir ini, pembahasan disajikan dalam enam bab dengan sistematika pembahasan sebagai berikut :

BAB I PENDAHULUAN

Berisi latar belakang yang menjelaskan tentang tugas akhir yang dilakukan, rumusan masalah, tujuan, manfaat dan sistematika penulisan yang digunakan dalam laporan kerja praktek ini.

BAB II TINJAUAN PUSTAKA

Berisi tentang materi-materi penunjang pengerjaan tugas akhir tersebut.

BAB III PERANCANGAN

Berisi tentang perancangan tugas akhir dari berupa sebuah diagram alur serta penjelasan proses addons tersebut berjalan.

BAB IV IMPLEMENTASI

Berisi tentang implementasi addons yang telah dikerjakan sebelumnya yang didalamnya berisi tentang interface dan beberapa potongan coding program.

BAB V PENGUJIAN DAN ANALISA

Pada bab ini akan dijelaskan tentang skenario penyerangan terhadap addons vulnerability scanner pada sebuah website yang diduga memiliki kelemahan dan memiliki celah untuk di hack.

BAB VI PENUTUP

Bab ini berisi tentang kesimpulan yang dapat diambil dari keseluruhan isi dari laporan dan tugas akhir serta Saran yang disampaikan penulis demi kesempurnaan sistem yang lebih baik.

DAFTAR PUSTAKA

Pada bagian ini akan dipaparkan tentang sumber-sumber literatur yang digunakan dalam pembuatan laporan ini.